

Nonlinear entanglement witnesses

Otfried Gühne¹ and Norbert Lütkenhaus^{2,3}

¹*Institut für Quantenoptik und Quanteninformation,
Österreichische Akademie der Wissenschaften, 6020 Innsbruck, Austria*
²*Quantum Information Theory Group, Institut für Theoretische Physik I,
and Max-Planck Research Group, Institute of Optics, Information and Photonics,
Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*
³*Institute for Quantum Computing, University of Waterloo,
200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada*
 (Dated: February 9, 2008)

Entanglement detection typically relies on linear inequalities for mean values of certain observables (entanglement witnesses), where violation indicates entanglement. We provide a general method to improve any of these inequalities for bipartite systems via nonlinear expressions. The nonlinearities are of different orders and can be directly measured in experiments, often without any extra effort.

PACS numbers: 03.65.-w, 03.65.Ud, 03.67.-a

Entanglement detection is one of the fundamental problems in quantum information science. On the one hand, it is crucial for experiments, since the question whether a produced state is entangled or not may decide whether a given experiment has been successful or not. On the other hand, it is also a challenging task for theoreticians, since the separability problem is, despite a lot of progress in the last years, essentially not solved.

In most of the experiments, so called entanglement witnesses are used for entanglement verification [1, 2, 3, 4, 5, 6, 7]. These are linear inequalities for mean values of certain observables, if the inequality is violated, the state must be entangled. For instance, Bell inequalities are such linear inequalities and may hence be viewed as entanglement witnesses. The question whether one can use *nonlinear* inequalities for entanglement detection has also been discussed and many nonlinear criteria are known [8, 9, 10, 11, 12, 13].

In this situation it is natural to ask whether it is possible to improve a given linear witness by some nonlinear expression. For discrete systems two examples for such an improvement are known. Uffink showed that certain Bell inequalities can be improved by nonlinear expressions [9]. Recently, Hofmann and Takeuchi proposed separability conditions called “local uncertainty relations” [10], which can improve witnesses in some cases [11]. For continuous variable systems it is known how to summarize certain families of linear inequalities to a single nonlinear one [12].

In this Letter we provide a method which allows to improve *all* entanglement witnesses for discrete bipartite systems by nonlinear expressions. Surprisingly, this works also for optimal entanglement witnesses, that is, witnesses where no other linear witness is stronger. Due to the simplicity of our method the nonlinear witnesses may be used from the beginning, without considering linear witnesses anymore. Our method allows to calculate such nonlinear witnesses to an arbitrary order. We dis-

cuss in detail the strength of our constructions for the case of two qubits. Interestingly, when implemented in an experiment, the nonlinear expressions in our constructions often require measurement of the same observables as the original witness. This allows for an improved entanglement detection without any extra effort.

Without losing generality, we consider witnesses \mathcal{W} as observables with a positive mean value on all separable states, thus a negative expectation value signals the presence of entanglement. Our aim is to find a nonlinear witness \mathcal{F} as a functional of the type $\mathcal{F}(\varrho) = \text{Tr}(\mathcal{W}\varrho) - \mathcal{X}(\varrho)$ which still should be positive on all separable states. Typically, the nonlinearity $\mathcal{X}(\varrho)$ will be a quadratic polynomial of certain expectation values. We consider only $\mathcal{F}(\varrho)$ which are *strictly stronger* than the witness \mathcal{W} . That is, we require that $\mathcal{F}(\varrho)$ detects all the states that are detected by \mathcal{W} and some states in addition.

Let us explain the main idea for the case of witnesses coming from the separability criterion of the positivity of the partial transpose (PPT) [14]. By definition, a quantum state ϱ shared between Alice and Bob is separable if it can be written as a mixture of product states, that is

$$\varrho = \sum_i p_i \varrho_i^A \otimes \varrho_i^B, \quad (1)$$

where $p_i \geq 0$ and $\sum_i p_i = 1$. Then, given a quantum state $\varrho = \sum_{ij,kl} \varrho_{ij,kl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ its partial transpose with respect to Bob’s system is defined as $\varrho^{T_B} = \sum_{ij,kl} \varrho_{ij,lk} |i\rangle\langle j| \otimes |k\rangle\langle l|$. If ϱ is a separable state, it can be easily seen that the partial transpose is positive, $\varrho^{T_B} \geq 0$. Thus, if for a state the partial transpose is not positive (ϱ is NPT), the state must be entangled. Indeed, it has been shown [4] that for 2×2 and 2×3 systems a state is PPT if and only if it is separable, while for other dimensions there are also PPT entangled states.

For any NPT state ϱ_0 we find that $\varrho_0^{T_B}$ has a negative eigenvalue λ_- and a corresponding eigenvector $|\phi\rangle$. An

entanglement witness for this state is then

$$\mathcal{W} = |\phi\rangle\langle\phi|^{T_B}. \quad (2)$$

Indeed, due to the identity $\text{Tr}(XY^{T_B}) = \text{Tr}(X^{T_B}Y)$ for arbitrary matrices X, Y , we have $\text{Tr}(\varrho_0\mathcal{W}) = \lambda_- < 0$ while for separable (and hence PPT) states $\text{Tr}(\varrho\mathcal{W}) = \langle\phi|\varrho^{T_B}|\phi\rangle \geq 0$ holds. Note that the witness in Eq. (2) is by no means specific: since the PPT criterion is necessary and sufficient for low dimensions, witnesses of this type suffice to detect all states in these systems. Furthermore, such witnesses can be shown to be optimal [5].

To improve the witness from Eq. (2) with nonlinear terms, first note that a functional like $\langle X\rangle\langle X^\dagger\rangle$ is convex (see Lemma 1 in Ref. [13]). This implies that a functional like $\mathcal{G} = \langle A\rangle - \sum_i \alpha_i \langle X_i\rangle\langle X_i^\dagger\rangle$ is concave in the state. That is, if $\varrho = \sum_k p_k \varrho_k$ is a convex combination of some states, then $\mathcal{G}(\varrho) \geq \sum_k p_k \mathcal{G}(\varrho_k)$.

Let us assume that we have chosen $A = |\phi\rangle\langle\phi|$, $X_i = |\phi\rangle\langle\psi_i|$ for an arbitrary $|\psi_i\rangle$ and take a separable state ϱ . Then ϱ^{T_B} is again separable and can be written as a convex combination of product states, $\varrho^{T_B} = \sum_k p_k |a_k b_k\rangle\langle a_k b_k|$. For $|\chi\rangle = |a_k b_k\rangle$ we have

$$\mathcal{G}(|\chi\rangle\langle\chi|) = \langle\chi|\phi\rangle\langle\phi|\chi\rangle \cdot \underbrace{\left[1 - \sum_i \alpha_i \langle\chi|\psi_i\rangle\langle\psi_i|\chi\rangle\right]}_{=: P(\chi)}. \quad (3)$$

Thus, if the polynomial $P(\chi)$ is positive on all product states, by concavity the functional \mathcal{G} is positive on all separable ϱ^{T_B} . Then, with the chosen X_i ,

$$\mathcal{F} = \langle|\phi\rangle\langle\phi|^{T_B}\rangle - \sum_i \alpha_i \langle X_i^{T_B}\rangle\langle (X_i^{T_B})^\dagger\rangle \quad (4)$$

is a nonlinear improvement of the witness $\mathcal{W} = |\phi\rangle\langle\phi|^{T_B}$. It is important to note that a term like $\langle X^{T_B}\rangle\langle (X^{T_B})^\dagger\rangle$ in Eq. (4) is easily accessible in experiments, even if X^{T_B} is non-Hermitian. Namely, we can write $X^{T_B} = H + i \cdot A$ as a sum of its Hermitian and anti-Hermitian part, where H and A are Hermitian. Then $\langle X^{T_B}\rangle\langle (X^{T_B})^\dagger\rangle = \langle H\rangle^2 + \langle A\rangle^2$ holds. With this method, we have:

Observation 1. (a) Let $\mathcal{W} = |\phi\rangle\langle\phi|^{T_B}$ be an entanglement witness. We define $X_i = |\phi\rangle\langle\psi_i|$ for an arbitrary $|\psi_i\rangle$ and $s(\psi)$ as the square of the largest Schmidt coefficient of $|\psi\rangle$. Then

$$\mathcal{F}^{(1)}(\varrho) = \langle|\phi\rangle\langle\phi|^{T_B}\rangle - \frac{1}{s(\psi)} \langle X^{T_B}\rangle\langle (X^{T_B})^\dagger\rangle \quad (5)$$

is a nonlinear improvement of \mathcal{W} .

(b) If we define $X_i = |\phi\rangle\langle\psi_i|$, $i = 1, \dots, K$ with an orthonormal basis $|\psi_i\rangle$, then

$$\mathcal{F}^{(2)}(\varrho) = \langle|\phi\rangle\langle\phi|^{T_B}\rangle - \sum_{i=1}^K \langle X_i^{T_B}\rangle\langle (X_i^{T_B})^\dagger\rangle \quad (6)$$

is also a nonlinear witness.

Proof. (a) The squared overlap between a state $|\psi\rangle$ and a product state is bounded by the maximal squared Schmidt coefficient [2], thus $P(\chi)$ in Eq. (3) is positive. (b) For the $|\psi_i\rangle$ we have in Eq. (3) $\sum_i \langle\chi|\psi_i\rangle\langle\psi_i|\chi\rangle = \text{Tr}(|\chi\rangle\langle\chi|) = 1$ which proves the claim. \square

This Observation provides a whole class of nonlinear improvements, one may pick an arbitrary $|\psi\rangle$ and compute the corresponding nonlinearity. In special situations one can also adjust the improvement: if an experiment produces the state $\varrho(p) = p\varrho_e + (1-p)\varrho_n$, which is a mixture of an entangled ϱ_e and some noise ϱ_n , a given witness may detect the states only for $p > p_{\text{crit}}$, i.e., $\text{Tr}(\mathcal{W}\varrho(p_{\text{crit}})) = 0$. Now one can choose the $|\psi\rangle$ in a way that the nonlinear terms are large at $\varrho(p_{\text{crit}})$, which leads to a significant improvement of the witness for the states of interest. Concerning the strength of the nonlinear improvements we can state:

Observation 2. (a) Let $\mathcal{W} = |\phi\rangle\langle\phi|^{T_B}$ be a witness. A state ϱ can be detected by a witness of the type $\mathcal{F}^{(1)}$ from Eq. (5) if and only if

$$\langle\phi|\varrho^{T_B}|\phi\rangle < \left[\text{Tr}_B \left(\sqrt{\text{Tr}_A(\varrho^{T_B}|\phi\rangle\langle\phi|\varrho^{T_B})} \right) \right]^2. \quad (7)$$

(b) A state can be detected by a witness of the type $\mathcal{F}^{(2)}$ from Eq. (6) if and only if

$$\langle\phi|\varrho^{T_B}|\phi\rangle < \langle\phi|(\varrho^{T_B})^2|\phi\rangle \quad (8)$$

holds. In this case, the state is detected by all nonlinear witnesses of the type $\mathcal{F}^{(2)}$.

(c) If Eq. (8) is fulfilled, then also Eq. (7) holds, thus the witnesses of the type $\mathcal{F}^{(1)}$ are stronger. Furthermore, Eqs. (7, 8) are never fulfilled for PPT states.

Proof. The proof is given in the Appendix. \square

Let us add that with the same idea also witnesses with higher nonlinearities, e.g. of fourth order, can be derived. To do so, note first that functionals like $\mathcal{G} = \langle A\rangle - \alpha\langle B\rangle\langle B^\dagger\rangle - \beta\langle C\rangle^2\langle C^\dagger\rangle^2$ are also concave in the state. If we choose $A = |\phi\rangle\langle\phi|$, $B = |\phi\rangle\langle\psi_1|$, $C = |\phi\rangle\langle\psi_2|$, we arrive at a similar expression as in Eq. (3). Now, $P(\chi)$ is a polynomial of fourth order that has to be positive on all product states [15].

To give an example which we will investigate later, let us assume that $|\psi_1\rangle, |\psi_2\rangle$ and $|\phi\rangle$ form an orthonormal set, where the biggest squared Schmidt coefficient from $|\psi_1\rangle, |\psi_2\rangle$ is $1/2$ and the one from $|\phi\rangle$ is $s_\phi \geq 1/2$. Then,

$$\begin{aligned} \mathcal{F}^{(3)} = & \langle|\phi\rangle\langle\phi|^{T_B}\rangle - \left(2 - \frac{2}{27s_\phi}\right) \cdot \langle B^{T_B}\rangle\langle (B^{T_B})^\dagger\rangle \\ & - \frac{2}{s_\phi} \langle C^{T_B}\rangle^2 \langle (C^{T_B})^\dagger\rangle^2 \end{aligned} \quad (9)$$

is a nonlinear witness of fourth order. The positivity of the polynomial $P(\chi)$ can directly be checked.

It should, however, be noted that higher orders do not necessarily provide witnesses, which are much stronger

than the witnesses with quadratic nonlinearity. The reason is that we are not trying to approximate the curvature of the convex set of separable states (in which case higher polynomials would be clearly an advantage): in our approach, we also require the concave functional to be positive on the convex set of separable states which makes the situation more complicated.

Let us discuss an application to two-qubit systems. A generic optimal witness for a two-qubit system is

$$\mathcal{W}(\alpha) = |\phi(\alpha)\rangle\langle\phi(\alpha)|^{T_B}, \quad (10)$$

$$|\phi(\alpha)\rangle = \cos(\alpha)|00\rangle + \sin(\alpha)|11\rangle. \quad (11)$$

It is useful to express all quantities directly in expectation values for observables. We use the abbreviations $s = \sin(\alpha)$, $c = \cos(\alpha)$, $s_2 = \sin(2\alpha)$, $c_2 = \cos(2\alpha)$ and $x_1x_2 = \langle\sigma_x \otimes \sigma_x\rangle$, $y_1 = \langle\sigma_y \otimes \mathbb{1}\rangle$ etc. here. The witness is then

$$\langle\mathcal{W}\rangle = \frac{1}{4}(1 + z_1z_2 + s_2(x_1x_2 + y_1y_2) + c_2(z_1 + z_2)). \quad (12)$$

To construct improvements, we choose the four vectors $|\psi_{1/2}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\psi_{3/4}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$, where the upper signs hold for $i = 1, 3$, and compute the corresponding $X_i = |\phi(\alpha)\rangle\langle\psi_i|$, which leads to the four nonlinear correction terms $\mathcal{X}_i := \langle X_i^{T_B} \rangle \langle (X_i^{T_B})^\dagger \rangle$ with

$$\begin{aligned} \mathcal{X}_{1/2} &= \frac{1}{32}[(c \pm s)(1 \pm x_1x_2 \pm y_1y_2 + z_1z_2) \\ &\quad + (c \mp s)(z_1 + z_2))^2 + ((c \mp s)(x_1y_2 - y_1x_2))^2], \\ \mathcal{X}_{3/4} &= \frac{1}{32}[(c \pm s)(x_1 \pm x_2) + (c \mp s)(z_1x_2 \pm x_1z_2))^2 \\ &\quad + ((c \mp s)(y_1 \mp y_2) + (c \pm s)(y_1z_2 \mp z_1y_2))^2]. \end{aligned} \quad (13)$$

With these nonlinearities, the nonlinear witnesses $\mathcal{F}^{(1)}$, $\mathcal{F}^{(2)}$, and $\mathcal{F}^{(3)}$ according to Eqs. (5, 6, 9) can directly be written down. Note that, especially for $c = \pm s$, several quadratic terms in the \mathcal{X}_i can be measured with the same measurements as in Eq. (12). Thus their implementation requires no extra effort.

To investigate the power of these new criteria, we consider the family of states $\varrho(\alpha) = (\mathbb{1} - |\phi(\alpha)\rangle\langle\phi(\alpha)|^{T_B})/3$, which are separable, but they lie on the boundary of the set of separable states, since $\text{Tr}(\mathcal{W}(\alpha)\varrho(\alpha)) = 0$. For different α we generate randomly states ϱ_r with $\|\varrho(\alpha) - \varrho_r\| \leq 0.2$ in Hilbert Schmidt norm [16]. For the entangled states in this ball we determine the probability of detecting it via the witness $\mathcal{W}(\alpha)$ and via a nonlinear criterion. First, we consider $\mathcal{F}^{(1)}$ as in Eq. (5), using $|\psi_2\rangle$ and $2 \cdot \mathcal{X}_2$. Then, we consider $\mathcal{F}^{(2)}$ as in Eq. (6), using all nonlinearities. We also test the criterion in Eq. (7), corresponding to all possible $\mathcal{F}^{(1)}$. Finally, we investigate $\mathcal{F}^{(3)}$ from Eq. (9) using $|\psi_3\rangle, |\psi_4\rangle$ and $s_\phi = c^2$. The results are shown in Fig. 1. Clearly, the nonlinear criteria improve the witness significantly [17].

Let us now discuss generalizations of our approach to other entanglement witnesses, which are not related

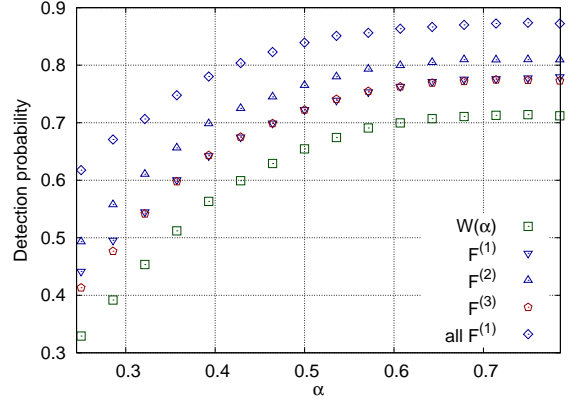


FIG. 1: Probability of detecting a state with a witness and with nonlinear criteria. See text for details.

to the PPT criterion. This can be done via *positive maps* [18]. Let \mathcal{H}_B and \mathcal{H}_C be Hilbert spaces and let $\mathcal{B}(\mathcal{H}_i)$ denote the linear operators on it. A linear map $\Lambda : \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_C)$ fulfilling $\Lambda(X) \geq 0$ for $X \geq 0$ and $\Lambda(X^\dagger) = \Lambda(X)^\dagger$ is called *positive* (P). A positive map is *completely positive* (CP) when for an arbitrary \mathcal{H}_A the map $\mathbb{I}_A \otimes \Lambda$ is P, otherwise, it is positive, but not completely positive (PnCP). Here, \mathbb{I}_A denotes the identity on $\mathcal{B}(\mathcal{H}_A)$. For example, the transposition is PnCP: While $X \geq 0$ implies $X^T \geq 0$ the partial transposition does not preserve the positivity of a state.

Indeed, it has been shown [4, 18] that a state $\varrho \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$ is separable iff for all P maps Λ the relation $\mathbb{I}_A \otimes \Lambda(\varrho) \geq 0$ holds. Consequently, if ϱ is entangled there must be a trace decreasing PnCP map Λ where $\mathbb{I}_A \otimes \Lambda(\varrho)$ has a negative eigenvalue λ_- and a corresponding eigenvector $|\phi\rangle$. Taking $(\mathbb{I}_A \otimes \Lambda)^\dagger$ as the adjoint of the map $(\mathbb{I}_A \otimes \Lambda)$ with respect to the scalar product $\text{Tr}(X^\dagger Y)$ a witness detecting ϱ is given by

$$\mathcal{W} = (\mathbb{I}_A \otimes \Lambda)^\dagger(|\phi\rangle\langle\phi|), \quad (14)$$

since we have $\text{Tr}[\varrho\mathcal{W}] = \text{Tr}[\varrho(\mathbb{I}_A \otimes \Lambda)^\dagger(|\phi\rangle\langle\phi|)] = \text{Tr}[\mathbb{I}_A \otimes \Lambda(\varrho)|\phi\rangle\langle\phi|] = \lambda_-$. Replacing the partial transposition by the map $(\mathbb{I}_A \otimes \Lambda)^\dagger$ this witness can then be improved as in Observation 1.

For an arbitrary witness, we make use of the Jamiolkowski isomorphism [18, 19] between operators and maps. According to this, an operator E on $\mathcal{B}(\mathcal{H}_B) \otimes \mathcal{B}(\mathcal{H}_C)$ corresponds to a map $\varepsilon : \mathcal{B}(\mathcal{H}_B) \rightarrow \mathcal{B}(\mathcal{H}_C)$ acting as $\varepsilon(\varrho) = \text{Tr}_B(E\varrho^T \otimes \mathbb{1}_C)$. Conversely, we have $E = (\mathbb{I}_{B'} \otimes \varepsilon)(|\phi^+\rangle\langle\phi^+|)$ where $\mathcal{H}_{B'} \cong \mathcal{H}_B$ and $|\phi^+\rangle = \sum_i |ii\rangle$ is a maximally entangled state on $\mathcal{H}_{B'} \otimes \mathcal{H}_B$. The key point is that if E is an entanglement witness, then ε is a PnCP map [18, 20]. Hence, any witness can be written as in Eq. (14) and finally we have:

Theorem 1. Any bipartite entanglement witness can be improved by nonlinear corrections using the methods of Observation 1.

In conclusion, we have shown that all bipartite entanglement witnesses can be improved by nonlinear expressions. These nonlinear witnesses are straightforward to calculate and can also be directly implemented in experiments, often without any extra effort. It is tempting to extend these constructions to the multipartite scenario. Here, this challenge remains undone.

We thank H.J. Briegel, M. Curty, J. Eisert, P. Hyllus, B. Kraus, M. Lewenstein, M. Piani and G. Tóth for discussions. This work has been supported by the FWF, the DFG (Emmy-Noether-Programm) and the EU (OLAQI, PROSECCO, QAP, QUPRODIS, SCALA).

Appendix — Here we prove Observation 2. (a) First, note that $Y = \varrho^{T_B}|\phi\rangle\langle\phi|\varrho^{T_B} =: |\eta\rangle\langle\eta|$ is projector onto a not normalized state $|\eta\rangle$. To derive a criterion for the strength of $\mathcal{F}^{(1)}$ we have to maximize $\langle X^{T_B} \rangle \langle (X^{T_B})^\dagger \rangle / s(\psi) = \langle \psi|\eta\rangle\langle\eta|\psi\rangle / s(\psi)$ for a given $|\eta\rangle$ over all $|\psi\rangle$. Let $|\eta\rangle = \sum_i a_i |ii\rangle$ and $|\psi\rangle = \sum_i b_i |\tilde{i}\tilde{i}\rangle$ be the Schmidt decompositions of $|\eta\rangle$ and $|\psi\rangle$, with decreasingly ordered Schmidt coefficients. We first show that for fixed Schmidt coefficients b_i it is optimal to take $|\tilde{i}\tilde{i}\rangle = |ii\rangle$. We have $|\langle\eta|\psi\rangle| = |\sum_{ij} a_i b_j \langle ii|\tilde{j}\tilde{j}\rangle| = |\sum_{ij} a_i b_j U_{ij}^A U_{ij}^B|$ where $U_{ij}^A = \langle i|\tilde{j}\rangle^A$ and $U_{ij}^B = \langle i|\tilde{j}\rangle^B$ are unitary. Defining $\mathbf{a}_{ij} = \sqrt{a_i}\sqrt{b_j}U_{ij}^A$ and $\mathbf{b}_{ij} = \sqrt{a_i}\sqrt{b_j}U_{ij}^B$ this can be written as a scalar product which is maximal, when $\mathbf{a}_{ij}, \mathbf{b}_{ij}$ are parallel. Due to the Cauchy-Schwarz inequality, we can then assume without losing generality $|\langle\eta|\psi\rangle| \leq \sum_{ij} a_i b_j |U_{ij}^A|^2$. Since U_{ij}^A is unitary, $|U_{ij}^A|^2$ is doubly stochastic, i.e. its row and column sums equal one. Due to Birkhoff's theorem [21] it can be written as a convex combination of permutation matrices. For a permutation π we have $\sum_i a_i b_{\pi(i)} \leq \sum_i a_i b_i$ due to the ordering of the a_i and b_j . This implies finally $|\langle\eta|\psi\rangle| \leq \sum_i a_i b_i$ where equality is achieved when $|\tilde{i}\tilde{i}\rangle = |ii\rangle$. Having fixed $|\tilde{i}\tilde{i}\rangle = |ii\rangle$ we only have maximize $\sum_i (b_i/b_0)a_i$ over all b_i . This is maximal when $(b_i/b_0) = 1$ for all i , which corresponds to a maximally entangled $|\psi\rangle = 1/\sqrt{d}\sum_i |ii\rangle$. But then $\langle\psi|\eta\rangle\langle\eta|\psi\rangle/s(\psi) = (\sum_i a_i)^2$ corresponds to the right hand side of Eq. (7). (b) First, note that for an arbitrary basis $|\psi_i\rangle$ in Eq. (6) $\sum_{i=1}^K \langle X_i^{T_B} \rangle \langle (X_i^{T_B})^\dagger \rangle = \text{Tr}(Y) = \langle\phi|(\varrho^{T_B})^2|\phi\rangle$. This shows Eq. (8). (c) Assume that ϱ fulfills Eq. (8). Since Y is of rank one, there is a single $|\psi'\rangle$ such that $\text{Tr}(Y) = \langle\psi'|Y|\psi'\rangle$. So, if we take $X = |\phi\rangle\langle\psi'|$ then the witness $\mathcal{F} = \langle|\phi\rangle\langle\phi|^{T_B} - \langle X^{T_B} \rangle \langle (X^{T_B})^\dagger \rangle$ detects ϱ . The witness $\mathcal{F}' = \langle|\phi\rangle\langle\phi|^{T_B} - \langle X^{T_B} \rangle \langle (X^{T_B})^\dagger \rangle / s(\psi')$ is stronger, and detects it as well. Finally, we have to show that Eq. (7) is never valid for a PPT state ϱ . In view of the proof of (a), it suffices to show $Q := \langle\phi|\varrho^{T_B}|\phi\rangle - \langle\psi|\varrho^{T_B}|\phi\rangle\langle\phi|\varrho^{T_B}|\psi\rangle/s(\psi) \geq 0$ for arbitrary $|\phi\rangle$ and maximally entangled $|\psi\rangle$. Since $\varrho^{T_B} \geq 0$ we can define $R = \sqrt{\varrho^{T_B}}|\phi\rangle\langle\phi|\sqrt{\varrho^{T_B}}$ and $S = \sqrt{\varrho^{T_B}}|\psi\rangle\langle\psi|\sqrt{\varrho^{T_B}}/s(\psi)$, then $Q = \text{Tr}(R) - \text{Tr}(RS) = \text{Tr}(R(\mathbb{1} - S))$. Since $R \geq 0$ and $S \geq 0$ it suffices to show that $\text{Tr}(S) < 1$, then $(\mathbb{1} - S) \geq 0$ follows and finally $Q \geq 0$. We have

$\text{Tr}(S) = \langle\psi|\varrho^{T_B}|\psi\rangle/s(\psi)$. Now, we use the known fact that a witness like $\mathcal{W} = s(\psi)\mathbb{1} - |\psi\rangle\langle\psi|$ where $|\psi\rangle$ is maximally entangled, detects no PPT states [6]. Since ϱ^{T_B} is PPT, this implies that $\text{Tr}(S) < 1$. \square

-
- [1] For experiments using witnesses see [2] and M. Barbieri *et al.*, Phys. Rev. Lett. **91**, 227901 (2003); K.J. Resch, P. Walther and A. Zeilinger, *ibid.* **94**, 070402 (2005); J. Altepeter *et al.*, *ibid.* **95**, 033601 (2005); H. Mikami *et al.*, *ibid.* **95**, 150404 (2005); N. Kiesel *et al.*, *ibid.* **95**, 210502 (2005); D. Leibfried *et al.*, Nature (London) **438**, 639 (2005); H. Häffner *et al.*, *ibid.* **438**, 643 (2005).
 - [2] M. Bourennane *et al.*, Phys. Rev. Lett. **92**, 087902 (2004).
 - [3] For theoretical studies see [4, 5, 6, 7] and B. Terhal, Phys. Lett. A **271**, 319 (2000); D. Bruß *et al.*, J. Mod. Opt. **49**, 1399 (2002); G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005); F. Brandão, Phys. Rev. A **72**, 022310 (2005).
 - [4] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
 - [5] M. Lewenstein *et al.*, Phys. Rev. A **62**, 052310 (2000).
 - [6] A. Sanpera, D. Bruß, and M. Lewenstein, Phys. Rev. A **63**, 050301 (2001).
 - [7] M. Lewenstein *et al.*, Phys. Rev. A **63**, 044304 (2001).
 - [8] L. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000); N. Korolkova *et al.*, Phys. Rev. A **65**, 052306 (2002); P. van Loock and A. Furusawa, *ibid.* **67**, 052315 (2003); G. Tóth, C. Simon, and J.I. Cirac, *ibid.* **68**, 062310 (2003); S. Yu *et al.*, Phys. Rev. Lett. **91**, 217903 (2003); E. Shchukin and W. Vogel *ibid.* **95**, 230502 (2005); F.A. Bovino *et al.*, *ibid.* **95**, 240407 (2005); A. Serafini, *ibid.* **96**, 110402 (2006).
 - [9] J. Uffink, Phys. Rev. Lett. **88**, 230406 (2002).
 - [10] H.F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).
 - [11] O. Gühne and M. Lewenstein, AIP Conf. Proc. **734**, 230 (2004); G. Tóth and O. Gühne, Phys. Rev. A **72**, 022340 (2005).
 - [12] V. Giovannetti *et al.*, Phys. Rev. A **67**, 022320 (2003); P. Hyllus and J. Eisert, New J. Phys. **8**, 51 (2006).
 - [13] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).
 - [14] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
 - [15] Note the similarity of this problem to J.K. Korbicz *et al.*, Phys. Rev. Lett. **94**, 153601 (2005).
 - [16] K. Życzkowski and H.-J. Sommers, J. Phys. A **34**, 7111 (2001).
 - [17] Note that from the local uncertainty relations [10] it follows that $\mathcal{F} = \langle\mathcal{W}(\pi/4)\rangle - [(x_1 + x_2)^2 + (y_1 + y_2)^2 + (z_1 + z_2)^2]/8$ is also an improvement of $\mathcal{W}(\pi/4)$ [11]. Using Eq. (6) one gets a similar expression $\mathcal{F}^{(2)}$, however, the numerics shows that $\mathcal{F}^{(2)}$ is slightly better than \mathcal{F} .
 - [18] For a review see M. Lewenstein, *Quantum information theory*, available at <http://www.itp.uni-hannover.de/tqowww/download.php>; M. Horodecki, P. Horodecki, and R. Horodecki, quant-ph/0109124.
 - [19] A. Jamiołkowski, Rep. Mat. Phys. **3**, 275 (1972).
 - [20] We assume without losing generality that ε^+ is trace decreasing, we can always rescale E to obtain this.
 - [21] See Theorem 8.7.1 in R.A. Horn and C.R. Johnson, *Ma-*

trix analysis (Cambridge University Press, 1999).